"UNDER SEAL"

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

UNITED STATES OF AMERICA,)	DOCKET NO. 3:17CR17-FDW
)	
v.)	SUPERSEDING BILL OF INDICTMENT
)	
(1) ADRIAN GENES,)	18 U.S.C. § 1344
a/k/a "tomuchdust," "DiAngelo,")	18 U.S.C § 1349
(2) DORIN MUNTEANU,)	18 U.S.C. § 2
a/k/a "Dorin Racu," and "neazugravu,")	
[redacted])	**FILED UNDER SEAL**
(4) ADRIAN MITAN,)	
a/k/a/ "Adi Calerderas," "Daucuvar,")	
"XPL," and "XPL.NY,")	
Defendants.)	

THE GRAND JURY CHARGES:

At all times relevant to this Indictment:

INTRODUCTION

1. From at least in or about May 2009 through in or about October 2010, in Mecklenburg County, within the Western District of North Carolina, and elsewhere, the defendants ADRIAN GENES, a/k/a "tomuchdust," and "DiAngelo," DORIN MUNTEANU, a/k/a "Dorin Racu," and "neazugravu," [redacted] ADRIAN MITAN, a/k/a/ "Adi Calerderas," "Daucuvar," "XPL," and "XPL.NY," and other persons known and unknown to the Grand Jury, engaged in bank fraud and conspiracy to commit bank fraud.

2. The Defendants participated in a "vishing" bank fraud scheme, further described below, using false and fraudulent pretenses, representations and promises, including:

a. tricking bank customers ("Vishing Victims") into submitting their debit card numbers and corresponding personal identification numbers ("PINs") to the Defendants using a network of compromised computers,

b. using the Vishing Victims' fraudulently-obtained debit card numbers re-encoded onto magnetic-stripe cards and corresponding PINs to obtain money, funds and credits under the custody and control of the Vishing Victims' banks and credit unions, and

c. tricking the Vishing Victims' banks and credit unions into believing that monetary withdrawals made from the Vishing Victims' bank and credit union accounts linked to Vishing Victims' debit cards had been made and authorized by the Vishing Victims, when in fact the Defendants, aiding and abetting each other, made the monetary withdrawals.

DEFENDANTS

3. ADRIAN GENES ("GENES"), who also used the alias names "tomuchdust" and "DiAngelo," was a Romanian national who resided in Galati, Romania and Spain. GENES was primarily responsible for: 1) making or causing to be made lists of telephone numbers of potential Vishing Victims, 2) conducting research to determine which bank and credit union customers were most likely to be vulnerable to the vishing bank fraud scheme, described below, and sharing that information with co-conspirators, 3) making or causing to be made lists of potentially vulnerable computers that hosted Internet Telephone systems, 4) compromising vulnerable computers hosting Internet Telephone systems and other vulnerable computers that were part of the technology infrastructure used to execute the vishing bank fraud scheme, 5) making or causing to be made vishing messages designed to trick Vishing Victims into believing the messages had been created by banks and credit unions, 6) initiating vishing campaigns, 7) collecting the debit card numbers and PINs input by Vishing Victims who responded to the vishing messages, 8) sending the fraudulently-obtained debit card numbers and PINs to co-conspirators for use in withdrawing money and funds from the associated accounts at automatic teller machines ("ATMs"), and 9) organizing and maintaining the technological infrastructure, computer code, and related data used to execute the vishing bank fraud scheme.

4. DORIN MUNTEANU ("MUNTEANU"), who also used the alias names "Dorin Racu," and "neazugravu," was a Romanian national who resided in Lafayette, Louisiana. MUNTEANU assisted in: 1) obtaining the fraudulently-obtained debit card numbers and PINs from GENES, 2) making or causing to be made magnetic-stripe cards re-encoded with the Vishing Victims' fraudulently-obtained debit card numbers, 3) traveling to ATMs and withdrawing money and funds from the bank and credit union accounts of the Vishing Victims, and 4) providing GENES with a percentage of the money and funds fraudulently obtained from the Vishing Victims' bank and credit union accounts.

[redacted]

6. ADRIAN MITAN ("MITAN"), who also used the alias names "Adi Calerderas," "Daucuvar," "XPL," and "XPL.NY," was a Romanian national who resided in New York, New York. MITAN assisted in: 1) sharing information about which bank or credit union customers

were vulnerable to the vishing bank fraud scheme, 2) compromising vulnerable computers hosting Internet Telephone systems, 3) initiating vishing campaigns, 4) providing technical advice to co-conspirators about how to increase the effectiveness of vishing campaigns, 5) collecting the debit card numbers and PINs input by Vishing Victims who responded to the vishing messages, 6) making or causing to be made magnetic-stripe cards re-encoded with the Vishing Victims' fraudulently-obtained debit card numbers, and 7) traveling to ATMs and withdrawing money and funds from the bank and credit union accounts of the Vishing Victims.

DEFINITIONS

7. As used in this Indictment,

a. "malware" is malicious software designed to execute multiple unauthorized operations on malware-infected computers, including control of compromised computers and fraudulent collection of debit card numbers and PINs from Vishing Victims for the vishing bank fraud scheme.

b. "money mules" are people who collect, retain and transfer fraudulently-obtained money and funds from the Vishing Victims' bank and credit union accounts

c. "Phishing" involves sending a fraudulent email purporting to be from a legitimate sender and designed to entice the recipient of the email to visit a fraudulent website where the recipient is tricked into disclosing personal information such as login information for email or financial accounts, or tricked into downloading malicious software when clicking a hyperlink contained in the email.

d. "VoIP" is an acronym for Voice over Internet Protocol. VoIP service allows voice telephone calls to be transmitted over the Internet instead of using traditional phone lines. A VoIP provider has paid subscribers whose calls are routed to the provider's servers via the Internet and then onto the telephone grid when necessary. The VoIP subscriber may use the VoIP provider's servers to provide telephone service, or may have VoIP software on their own servers that then connect to the VoIP provider in order to route calls onto the telephone network.

e. "Vishing" is a combination of "voice" and "phishing." Vishing uses voice recordings to communicate phishing messages, that is, messages that purport to be from legitimate sources, which in this Superseding Indictment were purported financial institutions.

f. "Banks and credit unions" are financial institutions as defined by Title 18, United States Code, Section 20.

THE VISHING BANK FRAUD SCHEME

8. From at least in or about May 2009 through in or about October 2010, in the Western District of North Carolina and elsewhere, the Defendants, using wire communications

and aiding and abetting each other and others known and unknown to the Grand Jury, engaged in a "vishing" bank fraud scheme and artifice to defraud and to obtain money, funds and credit of Vishing Victims, and to obtain money, funds and credits under the custody and control of Vishing Victims' financial institutions by: (1) secretly installing hidden malicious software ("malware") onto a network of compromised computers, (2) using the installed malware on the network of compromised computers to deceive and defraud Vishing Victims into providing the Defendants with the Vishing Victims' debit card numbers and personal identification numbers ("PINs"), (3) using the Vishing Victims' fraudulently-obtained debit card numbers and PINs to pose as the Vishing Victims, (4) under false pretenses, tricking the Vishing Victims' banks into believing that the Vishing Victim had requested monetary withdrawals or monetary transfers of funds from the Vishing Victims' bank and credit union accounts, and (5) making fraudulent, unauthorized withdrawals of money and funds out of the Vishing Victims' bank and credit union accounts.

MANNER AND MEANS

9. GENES and MITAN acquired and employed software tools to facilitate intrusions into computer systems. These software tools were designed to facilitate the intrusions into VoIP servers, including conducting searches to identify, locate and use vulnerable computers to execute the vishing bank fraud scheme.

10. GENES used multiple compromised computers as command and control ("C & C") computers for executing the vishing bank fraud scheme. One of GENES' C & C computers was located at an Internet hosting company in Columbus, Ohio, ("Columbus C & C"). The Columbus C & C computer contained software tools and scripts to execute the scheme, a map of compromised VoIP systems, vishing message audio files, bank and credit union names used in the vishing message audio files, telephone numbers for select area codes and information from approximately eight hundred (800) debit cards, including debit card numbers, PINs and card expiration dates fraudulently obtained from Vishing Victims.

11. GENES used the C & C compromised computer to connect to multiple compromised VoIP Gateway ("CVG") computers. One of the CVG computers used in the vishing bank fraud scheme was located at an IT services company in Charlotte, North Carolina ("Charlotte CVG"). GENES used the Charlotte CVG to make numerous VoIP telephone calls in an attempt to collect debit card numbers and PINs from potential Vishing Victims.

12. GENES and MITAN launched numerous vishing attacks from in or about May 2009 through in or about October 2010 using multiple C & C computers and multiple CVG computers, including the Columbus C & C and the Charlotte CVG computers.

13. In launching the vishing attacks, GENES and MITAN employed interactive voice response ("IVR") software to place telephone calls to a range of telephone numbers within specific area codes. When targeted Vishing Victims answered their telephones, the IVR software played digital audio files that falsely stated to the targeted Vishing Victims that there was a problem or issue with a payment card for their financial accounts at select banks or credit unions that maintained branch offices in locations corresponding with the targeted Vishing Victims' telephone area code. The digital audio file also instructed the targeted Vishing Victims to enter

their debit card numbers and corresponding PINs on their telephone keypad, falsely claiming that the debit card information was required to resolve the problem associated with the debit cards linked to the Vishing Victims' bank and credit union accounts.

14. During the vishing attacks, debit card numbers and PINs fraudulently obtained from Vishing Victims in response to the IVR system's prompts were recorded in text files automatically saved on compromised C & C computers and other compromised computers. GENES and MITAN accessed those text files maintained on compromised computers.

15. MUNTEANU [redacted] served as money mules. GENES often sent the Vishing Victims' fraudulently-obtained debit card information to MUNTEANU, [redacted] and others via Yahoo Instant Messenger or other Instant Messaging software programs.

16. MUNTEANU [redacted] used the Vishing Victims' fraudulently-obtained debit card information to fraudulently withdraw money and funds from the Vishing Victims' bank and credit union accounts, typically using ATMs.

17. Upon their successful withdrawal of money and funds from the Vishing Victims' bank and credit union accounts, MUNTEANU [redacted] retained a certain percentage of the fraudulently-obtained money and funds, and sent the remainder of those money and funds to GENES.

18. MITAN received the Vishing Victims' fraudulently-obtained debit card numbers and PINs from GENES and from text files on compromised computers. MITAN used the debit card information to fraudulently withdraw money and funds from the Vishing Victims' bank and credit union accounts, typically using ATMs.

19. The Defendants made or caused to be made magnetic-stripe cards re-encoded with the Vishing Victims' fraudulently-obtained debit card information. Thereafter, they used the re-encoded magnetic stripe cards at ATMs, and input the PINs on ATM keypads to fraudulently withdraw money and funds from the Vishing Victims' bank and credit union accounts.

COUNT ONE
(BANK FRAUD CONSPIRACY - 18 U.S.C. §1349)

20. Paragraphs 1 through 19 of this Superseding Bill of Indictment are re-alleged and incorporated herein by reference as though fully set forth herein.

21. From at least in or about May 2009 through in or about October 2010, in Mecklenburg County, within the Western District of North Carolina, and elsewhere, the defendants,

ADRIAN GENES, a/k/a "tomuchdust," and "DiAngelo,"
DORIN MUNTEANU, a/k/a "Dorin Racu," and " neazugravu,"
[redacted]
ADRIAN MITAN, a/k/a/ "Adi Calerderas," " Daucuvar," "XPL," and "XPL.NY,"

knowingly and intentionally conspired and agreed with each other, and with other persons known and unknown to the Grand Jury, to execute and attempt to execute a bank fraud scheme.

Object of the Conspiracy

22. It was an object of the conspiracy for the Defendants ADRIAN GENES, a/k/a "tomuchdust," and "DiAngelo," DORIN MUNTEANU, a/k/a "Dorin Racu," and "neazugravu," and [redacted] ADRIAN MITAN, a/k/a/ "Adi Calerderas," "Daucuvar," "XPL," and "XPL.NY," and other persons known and unknown to the Grand Jury, to unlawfully enrich themselves by executing a bank fraud scheme, a violation of Title 18, United States Code, Section 1344(2).

Manner and Means

23. The conspirators carried out the conspiracy in the manner and means described in paragraphs 9 through 19 of this Superseding Bill of Indictment, among others.

All in violation of Title 18, United States Code, Sections 1349.

COUNT TWO
(BANK FRAUD - 18 U.S.C. §1344(2))

24. Paragraphs 1 through 19 of this Superseding Bill of Indictment are re-alleged and incorporated herein by reference as though fully set forth herein.

23. From at least in or about May 2009 through in or about October 2010, in Mecklenburg County, within the Western District of North Carolina, and elsewhere, the defendants,

ADRIAN GENES, a/k/a "tomuchdust," and "DiAngelo,"
DORIN MUNTEANU, a/k/a "Dorin Racu," and " neazugravu,"
[redacted]
ADRIAN MITAN, a/k/a/ "Adi Calerderas," " Daucuvar," "XPL," and "XPL.NY,"

and others known and unknown to the Grand Jury, with the intent to defraud, did knowingly and intentionally execute and attempt to execute a scheme or artifice to obtain money under the custody and control of financial institutions, including but not limited to Bank of America, Wells Fargo Bank, Wachovia, Old Point National Bank, CDC Federal Credit Unions, NAE Federal Credit Unions, TIC Federal Credit Union and Bangor Savings Bank, by means of false and fraudulent pretenses, representations and promises, to wit, used fraudulently-obtained bank account numbers and personal identification numbers (PIN) of Vishing Victims to pose as the Vishing Victims and, under false pretenses, tricking the Vishing Victims' banks and credit unions into believing that the Vishing Victim had requested monetary withdrawals or monetary transfers

of funds in the Vishing Victims' bank accounts, and making fraudulent, unauthorized withdrawals and wire transfers of funds out of the Vishing Victims' bank accounts.

All in violation of Title 18, United States Code, Sections 1344(2) and 2.

NOTICE OF FORFEITURE AND FINDING OF PROBABLE CAUSE

Notice is hereby given of 18 U.S.C. §§ 981, 982, 1029, and 2323, 28 U.S.C. § 2461(c), and 21 U.S.C. § 853. Under Section 2461(c), criminal forfeiture is applicable to any offenses for which forfeiture is authorized by any other statute, including but not limited to 18 U.S.C. § 981 and all specified unlawful activities listed or referenced in 18 U.S.C. § 1956(c)(7), which are incorporated as to proceeds by Section 981(a)(1)(C). The following property is subject to forfeiture in accordance with Section 981, 982, 1029, 2323, 2461(c), and/or 853:

a. All property which constitutes or is derived from proceeds obtained directly or indirectly as a result of the violations set forth in this bill of indictment;

b. All property used, or intended to be used, in any manner or part to commit or facilitate the commission of the violations; and

c. If, as set forth in 21 U.S.C. § 853(p), any property described in (a), (b), or (c) cannot be located upon the exercise of due diligence, has been transferred or sold to, or deposited with, a third party, has been placed beyond the jurisdiction of the court, has been substantially diminished in value, or has been commingled with other property which cannot be divided without difficulty, all other property of the defendant/s to the extent of the value of the property described in (a), (b), and (c).

A TRUE BILL:

[redacted]

FOREPERSON

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY

THOMAS A. O'MALLEY
ASSISTANT U.S. ATTORNEY